REMARKS

Applicants have combined the elements of Claims 13, 14 and 15 into Claim 1. These claims have been canceled. The resulting method defines a system having novel and non-obvious elemnts and steps and should result in patenability thereof.

The Examiner is respectfully requested to reconsider the rejection of Claims 1, 2, 9 - 12, 14, and 16 - 20 under 35 U.S.C. §103(a) as being unpatentable over Levi (United States Patent 6,636,983) in view of Rowland, (United States Patent 6,405,318). In view of the cancellation of Claims 13 - 15 and the incorporation of them in Claim 1, the Examiner is respectfully requested to reconsider the rejection of Claims 13 and 15 under 35 U.S.C. §103(a) as being unpatentable over Levi (United States Patent 6,636,983) in view of Rowland, (United States Patent 6,405,318), and further in view of Lambert, et al. (United States Patent 6,367,016).

Levi discloses a device status tracking method to address the need for a uniform resource locator status tracking system. It involves installing a web exception sentinel on a monitor server and configuring the exception sentinel to monitor at least one uniform resource locator at a monitored web site. The method generates a virtual device identifier associated with at least one monitored uniform resource locator and retrieving, from the web site, the monitored uniform resource locator by the exception sentinel. It includes processing the retrieved uniform resource locator at the exception sentinel based on configuration data and communicating sentinel data to an operations center, the sentinel data being based on the retrieved uniform resource locator. Also, the method includes alerting, from the operations center, an alert contact in response to the retrieved uniform resource locator received at the operations center.

Levi also discloses a system for device status tracking to address the above-stated need, and uses a processor, a computer readable memory coupled to the processor and an application stored in the memory. The processor, when executing the application, is operable to install a web exception sentinel on a monitor server and configure the exception sentinel to monitor at least one uniform resource locator at a monitored web site. The processor, when executing the application, is further operable to generate a virtual device identifier associated with at least one monitored uniform resource locator and retrieve, from the web site, the monitored uniform

resource locator by the exception sentinel. The processor, when executing the application, is further operable to process the retrieved uniform resource locator at the exception sentinel based on configuration data and communicate sentinel data to an operations center, the sentinel data being based on the retrieved uniform resource locator. The processor, when executing the application, is further operable to alert, from the operations center, an alert contact in response to the retrieved uniform resource locator received at the operations center.

It is important to note that in implementing the Levi invention, the user must perform some initial positive action in order for the system to operate. Levi does not focus on "intrusion" in his invention. Levi discloses a monitoring system. The system monitors health indicative operating parameters based upon the operating system and the hardware used. A contact means is involved which represents one or more personnel who are contacted in order to respond and repair problems associated with the devices monitored by the remote monitoring system. The contact can be done by electronic mail, a pager, a phone, or a fax. This element is not found in Rowland or Lambert. To implement capability and session monitoring in accordance with the process, one must sign up for service to be rendered to him/her. The sign up is to acquire licenses for the system and is done using a web page. The invention is not used to detect an intrusion so there is no basis to combine this reference with Rowland.

Rowland, as the Examiner has stated, does provide a real-time intrusion detection method and system. The intrusion detection system automatically and dynamically builds user profile data (known as a signature) for each user (or alternatively, a class of users) that can be used to determine normal actions for each user to reduce the occurrence of false alarms and to improve detection. The user profile data (signature) is saved and updated every time the user logs on and off the system. The advantage of dynamically building user profile data based on past user behavior and comparing it to that user's current behavior is that the number of false alarms is reduced. In addition, there is no need to enter sets of rules prior to system initialization. The system detects suspicious actions, determines the source and institutes autonomous responses. The system acts to mitigate the effects of an intrusion and to prevent future actions without waiting for human action. The automatic actions to be taken can be specified by the system administrator prior to initialization of the system. The automatic actions can be tailored to

address the specific anomaly detected by the intrusion detection system. For example, through a local or system controller, the system can log the events, disable user accounts and block access to the system. In one embodiment, the system coordinates information transfer within host, multi-host and network environments to coordinate intrusion response. The system combines the above listed capabilities with real-time monitoring of log audit files, port scan detection.

The Lambert invention relates to the control of access to electronically provided services with its focus on the control of access to such services using tokens such as plastic cards. An example of the "service" intended by Lambert is the dispensing of cash by an automatic teller machine (ATM). Access to facilities provided by the ATM are typically controlled by requiring a user to present a personalized plastic card carrying data on a magnetic stripe to a card reader associated with the ATM. The user is required to key in a personal identification number (PIN) which is used by the system to access data in the card which together with data held in the system relating to the user enables the system to determine whether the requested transaction should be authorized. The "service" has been extended to many types of transactions including the purchase of goods in retail outlets, access to processes on computer networks and the provision of stockbroking services. Lambert saw a need for increased flexibility and security in the control of access through retail tills/terminals or ATM's. Lambert's services may only be accessed by authorised end-users with a valid card, at a valid till and, where appropriate, under the control of an authorised sales assistant or other operator. The system of Lambert provides an audit trail for each transaction to facilitate the detection of fraud and the settlement of any dispute that may arise from the transaction. An integral part of the invnetionis the use of the "smart card."

The method for controlling access to an electronically provided service of Lambert involves storing one or more application modules, which permit such a service to be delivered, in encrypted form so as to be accessible only under the control of a decryption key and, in response to a request for access to a particular service initiated by presentation of a token by a user, developing a decryption key from token data read from said token together with personal data provided by the user to provide access to the requested service decryption key, token reading means for accepting a token presented to the system by a user requiring access to a particular service or services, data receiving means for receiving personal data relating to the user, and a

key generator adapted to combine data stored in said token with data received by said data receiving means to generate a decryption key to by decryption of the associated application module.

To gain access to the system, Lambert does incorporate using personal data relating to the user such as a personal identification (PIN) number in which case the data receiving means will be a simple keypad. Alternatively, he does state that in a more advanced system, the data may be developed from biometric data read by a reader adapted to recognise particular facial or other characteristics of the user such as fingerprint or hand geometry. Lambert's use of the biometric data is totally different from the manner in which that data is used by Applicant. Lambert is using the data to gain access to the system to receive the service. Applicants are using the data, in combination with other elements to determine if an intrusion has occured.

There is no basis to combine these references with Lambert as Lambert discloses control of access to electronically provided services using plastic cards, that is a "smart card." The Lambert invention relates to providing services. There is no mention or even suggestion of the concept of preventing "intrusion" which is the objective of Rowland (and which is not the objective of Levi) nor the monitoring of health indicative operating parameters based upon the operating system and the hardware used as disclosed by Levi. Levi and Rowland are different species. Lambert uses the smart card to allow cash to be dispensed by an ATM, or it is used in retail outlets, stock brokerage transactions.

There are individual elements which are common to all three references, but there the similarity stops. Lambert is not directed toward the theft prevention of personal computers. Lambert does not disclose issuing an alarm to a central surveillance unit whenever a laptop is, without notice disconnected from a network.

In analyzing the Levi and Rowland references cited, it is questionable whether and why the skilled artisan would look to supplement the teaching of the Levi primary reference. The Examiner concedes that there are elements found in Applicants' claims which are not disclosed in Levi, Rowland and Lambert. To reiterate, in the rejection, the Examiner is selectively picking

and choosing individual elements disclosed in the references to the exclusion of what the three references as a whole teach to one skilled in the art.

The Examiner in his application of the cited references is improperly picking and choosing. The rejection is a piecemeal construction of the invention. Such piecemeal reconstruction of the prior art patents in light of the instant disclosure is contrary to the requirements of 35 U.S.C. § 103.

> The ever present question in cases within the ambit of 35 U.S.C. § 103 is whether the subject matter as a whole would have been obvious to one of ordinary skill in the art following the teachings of the prior art at the time the invention was made. It is impermissible within the framework of Section 103 to pick and choose from any one reference only so much of it as will support a given position, to the exclusion of other parts necessary to the full appreciation of what such reference fairly suggests to one of ordinary skill in the art. (Emphasis in original) In re Wesslau 147 U.S.P.Q. 391, 393 (CCPA 1965)

This holding succinctly summarizes the Examiner's application of references in this case, because the Examiner did in fact pick and choose so much of the Rowland and Lambert references to support the rejection and did not cover completely in the Office Action the full scope of what these varied disclosure references fairly suggest to one skilled in the art.

With respect to the combining of Claims 13 - 15 into Claim 1, the totality of the elements now present in Claim 1 are not anticipated nor rendered obvious by the combination of references cited. The Examiner is requested to allow this case as a result of the aforementioned Amendments to the claims and the cancellations thereof.

The Commissioner is requested to grant a one month extension within which to file this response to the above-noted Official Action. A check in the amount of $120.00 is enclosed to cover the extension fee of one month.

Respectfully Submitted,

Thomas A. Beck
Registration Number 20,816
26 Rockledge Lane
New Milford, CT 06776

I hereby certify that this paper is being mailed via the United States Postal Service, first class mail, on the date indicated below addressed to the Commissioner of Patents and Trademarks, Post Office Box 1450, Alexandria, VA 22313-1450

Signature _____ Date: January 20, 2006

Thomas A. Beck